AMENDMENTS TO THE CLAIMS

Please amend claims 1-10 as indicated below, and add new claims 11-20 as presented below.

Pursuant to 37 C.F.R. § 1.121 the following listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of the Claims:

Claim 1 (Currently Amended): A method for providing a time stamp by ~~means of~~ using a tamper-proof time signal ~~(5, 10)~~ via a telecommunications network ~~(2),~~ comprising the steps of:

receiving, at a central system, a request from a network user for a ~~wherein a network user (1a, 1b, . . . , 1c) requests an, in particular,~~ ~~officially recognized~~ time signal ~~(5, 10) from an, in particular, certified central system (3)~~;

encrypting said time signal ~~being encrypted~~ by the central system ~~(3)~~ with at least one key[[,]];

transmitting the encrypted time signal ~~transmitted~~ to the network user ~~(1a, 1b, . . . , 1c)~~ via the telecommunications network ~~(2) after encryption;, and~~

providing the ~~decrypted by this~~ network user with the same at least one key ~~or keys~~; and

synchronously generating, at the central system and the network user, the at least one key.

Claim 2 (Currently Amended): The method as recited in claim 1, wherein the synchronously generating is performed so as to change the at least one key~~, which is present at~~

~~both the network user (1a, 1b, . . . , 1c) and at a central system (3),~~ changes synchronously ~~at the network user and at the central system, especially~~ after predetermined time intervals.

Claim 3 (Currently Amended): The method as recited in claim 1, further comprising the steps of: ~~one of the preceding claims, wherein~~

providing the network user ~~(1a, 1b, . . . , 1c)~~ and the central system ~~(3) are each provided~~ each with at least one respective clock system ~~(4a, 4b, . . . , 4c, 6a, 6b, . . . , 6c)~~;

respectively assigning the at least one respective clock system at ~~each two of these clock systems (4a-6a, 4b-6b, . . . , 4c-6c) being assigned to each other and to~~ the network user ~~(1a, 1b, . . . , 1c)~~ to the at least one respective clock system at the central system so that the respectively assigned at least one respective clock system operate ~~and operating~~ synchronously to generate [[a]] the at least one key ~~which changes synchronously in time~~.

Claim 4 (Currently Amended): The method as recited in claim 1, further comprising the steps of: ~~one of the preceding claims,~~

receiving a time signal request, at the central system, from the ~~wherein when a~~ network user ~~(1a, 1b, . . . , 1c) requests a time signal (5, 10),~~; and

determining, by the central system, ~~(3) determines~~ a clock system ~~(4a, 4b, . . . , 4c)~~ assigned to ~~this~~ the network user using a transmitted identifier, ~~in particular,~~ wherein the transmitted identifier is the network address of the network user ~~(1a, 1b , . . . , 1c),~~; and wherein the at least one key is ~~encrypts the time signal (5, 10) with a key~~ generated by the assigned clock system ~~(4a, 4b, . . . , 4c) and/or with the identifier,~~[[,]] ~~and transmits it~~.

Claim 5 (Currently Amended): A method for transmitting data with a tamper-proof time stamp over a telecommunications network ~~(2)~~ from a first network user to a second network user, comprising the steps of:

obtaining ~~wherein the data, along with~~ a time signal ~~obtained~~ in accordance with a method as recited in claim 1; ~~one of the preceding claims,~~

transmitting the time signal and the data ~~is transmitted~~ from the first network user to the second network user one of directly and ~~or~~ indirectly via the central system ~~(3)~~.

Claim 6 (Currently Amended): The method as recited in claim 5, further comprising the steps of:

encrypting, by the first network user, at least one of ~~wherein~~ the data and/~~or~~ the time signal ~~is/are encrypted by the first network user (1a, 1b, . . . ,1c)~~ during transmission~~, especially with the key present at the central system (3) and at the first network user (1a, 1b, . . . , 1c) and/or with an identifier of the first network user (1a, 1b, . . . , 1c)~~.

Claim 7 (Currently Amended): The method as recited in claim 5, ~~one of claims 5 through 6,~~ wherein [[a]] the central system ~~(3)~~ is provided at the second network user.

Claim 8 (Currently Amended): The method as recited in claim 5, ~~one of claims 5 through 6, wherein~~ further comprising the step of returning, by the central system, ~~(3) returns~~ an acknowledgement of receipt~~, especially with a time signal (5, 10),~~ to the first network user ~~(1a, 1b, . . . , 1c)~~.

Claim 9 (Currently Amended): A system for generating a tamper-proof time stamp in network-based communication systems, ~~wherein~~ the system ~~includes~~ comprising:

a central system connected to the network-based communication system; ~~(3)~~

a network user connected to the network-based communication system; and

a respective ~~one each~~ clock system ~~(4a, 4b, . . . , 4c, 6a, 6b, . . . , 6c) on the side of~~ a at the network user ~~(1a, 1b, . . . , 1c)~~ and ~~on the side of~~ at the central system, ~~(3);~~ wherein each of the respective clock systems ~~(4a-6a, 4b-6b, . . . , 4c-6c) being~~ is assigned to each other ~~and to the network user (1a, 1b, . . . , 1c)~~ and ~~operating~~ configured to operate synchronously so as to generate [[a]] at least one changed key ~~which changes, in particular, at intervals of time,~~;

wherein the central system is configured to encrypt a ~~and with which an, in particular, officially recognized~~ time signal using the at least one changed key, and further configured to send the encrypted time signal to the network user; ~~(5, 10) can be encrypted in the central system (3)~~ and

~~decrypted by~~ wherein the network user is configured to decrypt the encrypted time signal ~~(1a, 1b, . . . , 1c) after it is sent to this network user~~.

Claim 10 (Currently Amended): The system as recited in claim 9, wherein the central system ~~(3) is formed by~~ includes a time signal transmitter ~~(5)~~.

Claim 11 (New): The method as recited in claim 1, further including the steps of:

providing the network user and the central system each with at least one respective clock system;

assigning the at least one respective clock system at the network user to the at least one respective clock system at the central system so that the assigned at least one respective clock system operate synchronously to change the at least one key.

Claim 12 (New): The method as recited in claim 6, wherein a central system is provided at the second network user.

Claim 13 (New): The method as recited in claim 6, wherein the central system is configured to return an acknowledgement of receipt to the first network user.

Claim 14 (New): The method as recited in claim 7, wherein the central system is configured to return an acknowledgement of receipt to the first network user.

Claim 15 (New): The method as recited in claim 1, further comprising the step of decrypting, by the network user using the at least one key, the transmitted encrypted time signal.

Claim 16 (New): The method as recited in claim 1, wherein the central system is a certified central system.

Claim 17 (New): The method as recited in claim 1, wherein the time signal is an officially recognized time signal.

Claim 18 (New): The method as recited in claim 4, wherein the at least one key is generated using at least one of the assigned clock system and the transmitted identifier.

Claim 19 (New): The method as recited in claim 9, wherein the at least one changed key is synchronously generated at intervals of time.

Claim 20 (New): The method as recited in claim 9, wherein the time signal is an officially recognized time signal.